

ASSESSMENT REPORT

~~OFFICIAL USE ONLY~~

Assessment of NRC's Wireless Devices

OIG-10-A-18 September 17, 2010



All publicly available OIG reports are accessible through
NRC's Web site at:
<http://www.nrc.gov/reading-rm/doc-collections/insp-gen/>

REPORT
for the
NUCLEAR REGULATORY COMMISSION
OFFICE OF THE INSPECTOR GENERAL

ASSESSMENT OF NRC'S WIRELESS DEVICES

Prepared by:

Southwest Research Institute®
P.O. Drawer 28510
San Antonio, Texas 78228-0510

Executive Summary

Background

The Nuclear Regulatory Commission (NRC) Office of the Inspector General (OIG) engaged Southwest Research Institute® (SwRI®) to perform a security assessment of the policy framework, technologies, vulnerabilities, and security controls for wireless access to specific NRC information systems at the One White Flint North (OWFN) and Two White Flint North (TWFN) facilities at NRC Headquarters in Rockville, MD. The two networks that SwRI evaluated were the Information Technology Infrastructure (ITI) and the Safeguards LAN-eSafe (SLES). SwRI's primary evaluation focused on two wireless access mechanisms: Internet-based wireless remote access to ITI using Blackberry handheld devices and Wi-Fi access to SLES. In addition, SwRI conducted a top-level overview of Bluetooth within OWFN and TWFN.

Purpose

The objective of this assessment was to determine if NRC's wireless devices meet their required operational capabilities and security requirements. Page B-6 of OIG's FY2010 Annual Plan includes more information about this assessment.

Results in Brief

The assessment identified one notable positive finding for SLES wireless security implementation and eight findings that require remediation. These eight findings relate to technical or procedural implementation and configuration of security controls for SLES wireless access. The findings indicate that although the wireless access system for SLES is well protected against penetration by an external attacker, the system is at risk for compromise by a motivated insider. Further, too much confidence is being placed in the effectiveness of existing security controls, and additional effort should be made to verify the effectiveness of these controls through monitoring and testing.

Additionally, the assessment identified three notable positive findings for ITI wireless security implementation and nine findings that require remediation. Two findings were related to missing or incomplete high-level policy, and seven findings were related to technical or procedural implementation and configuration of security controls for ITI wireless access. The findings indicate that ITI is well protected against external penetration and compromise of the Blackberry/Blackberry Enterprise Server (BES) architecture, and monitoring for unauthorized network-connected wireless access systems is effective. However, several unauthorized network-disconnected wireless access systems were identified during the assessment. Additional scrutiny should be placed on wireless detection of rogue access points that are not directly connected to ITI.

Multiple active Bluetooth devices were detected in OWFN and TWFN. The detected devices were predominantly Bluetooth-enabled cell phones, but several Bluetooth printers and mouse/keyboard sets were also detected. Existing policy requires that Bluetooth-enabled devices must be approved for use; and, according to impromptu interviews, there was no review and approval of these devices.

Finally, the overall policy framework that supports both SLES and ITI should be reviewed and revised. The existing policy framework is complex and confusing, and both gaps and overlaps exist. In addition, the traceability between high-level policies (such as the NRC Management Directives) and technical policies, procedures, and implementation guidelines for operation and configuration of IT systems is unclear.

Recommendations

This report makes 18 recommendations to address the security vulnerabilities that require remediation. A consolidated list of recommendations is on pages 13 - 14.

Agency Comments

At an exit conference held on September 7, 2010, agency management stated their general agreement with the findings and recommendations in this report. Agency management also provided supplemental information that has been incorporated into this report as appropriate. As a result, the agency opted not to provide formal comments for inclusion in this report.

TABLE OF CONTENTS

| | |
|---|----|
| Executive Summary | ii |
| 1. Background | 1 |
| 2. Purpose..... | 2 |
| 3. Findings - SLES | 3 |
| 4. Findings - ITI | 7 |
| 5. Observations | 12 |
| 6. Consolidated List of Recommendations | 13 |
| 7. Agency Comments | 15 |

APPENDIX

A. ASSESSMENT SCOPE AND METHODOLOGY

1. BACKGROUND

The Nuclear Regulatory Commission (NRC) Office of the Inspector General (OIG) engaged Southwest Research Institute® (SwRI®) to perform a security assessment of the policy framework, technologies, vulnerabilities, and security controls for wireless access to specific NRC information systems at the One White Flint North (OWFN) and Two White Flint North (TWFN) facilities at NRC Headquarters in Rockville, MD. The two networks that SwRI evaluated were the Safeguards LAN-eSafe (SLES) and the Information Technology Infrastructure (ITI). SwRI's primary evaluation focused on two wireless access mechanisms: Internet-based wireless remote access to ITI using BlackBerry handheld devices and Wi-Fi access to SLES. In addition, SwRI conducted a top-level overview of Bluetooth use within OWFN and TWFN.

BlackBerry handheld devices are mobile e-mail and smart phone platforms that use commercial cell phone communications channels and Internet connections to connect wirelessly to enterprise information resources. They are integrated into an organization's e-mail and file system with a software package called "BlackBerry Enterprise Server" (BES). ITI uses BES to provide remote wireless e-mail and file access to authorized users. The BES servers installed in the ITI infrastructure connect internally to information repositories such as file servers and Exchange e-mail servers and connect externally over an Internet connection to servers operated by the BlackBerry parent company, Research In Motion (RIM). The RIM servers connect to BlackBerry handhelds through Internet connections to cellular service providers and wireless connections to each individual handheld device.

Wi-Fi is a wireless local area network technology that uses the IEEE 802.11 communications standard to provide remote connectivity to an information system. A Wi-Fi enabled device, such as a desktop or laptop computer, mobile phone, or printer, can connect to an enterprise network and/or the Internet when within range of a wireless access point connected to the enterprise network. SLES uses a secured form of Wi-Fi to provide wireless access to the network. Wireless access points are connected to controller devices within the SLES infrastructure, which are in turn connected to eSafe information repositories. The wireless access points provide secure wireless network connections to wireless client computers within OWFN and TWFN.

Bluetooth is an open wireless technology standard for exchanging data over short distances from fixed and mobile devices and creating personal area networks (PANs). Bluetooth is used to provide connectivity for many types of devices, including smart phones, keyboards, mice and other pointing devices, printers, and laptop computers.

2. PURPOSE

The objective of this assessment was to determine if NRC's wireless devices meet their required operational capabilities and security requirements. Page B-6 of OIG's FY2010 Annual Plan includes more information about this assessment.

Appendix A provides a detailed description of the scope and methodology for this wireless assessment.

3. FINDINGS - SLES

The assessment identified one notable positive finding for SLES wireless security implementation and nine findings that require remediation. All nine findings requiring remediation related to implementation or configuration of security controls for SLES wireless access. The findings indicate that although the wireless access system for SLES is well protected against penetration by an external attacker, the system is at risk for compromise by a motivated insider. Further, too much confidence is being placed in the effectiveness of existing security controls, and additional effort should be made to verify the effectiveness of these controls through monitoring and testing. Specific findings for SLES are described below.

3.1 External Security for SLES Wireless Access Is Effective

Requirement

NIST SP 800-53, Control AC-17 requires that wireless remote access to NRC information systems be authorized, monitored, and controlled.

Finding

Wireless security for SLES is designed, configured, and managed to effectively prevent unauthorized external access to SLES 802.11 access points. The system uses FIPS 140-2 compliant components, does not broadcast service set identifier (SSID) information, uses strong encryption, and controls Wi-Fi signal radiation outside the OFWN and TWFN buildings.

3.2 Protection of the SLES Wireless Client BIOS Password and Wireless Client Solid State Drive Is Inadequate

Requirement

NIST SP 800-53, Control PE-3 Enhancement 1 requires that physical access to specific wireless devices be controlled independently of facility physical access.

Finding

Physical access to the internal components of SLES wireless clients is not controlled adequately. SLES wireless client computers can be easily disassembled, and the internal components can be exploited to compromise security. By removing the non-volatile random access memory (NVRAM) battery in the SLES wireless client for a short period of time, the basic input-output system (BIOS) password can be reset to the system default value. This default value is publicly available. By resetting the BIOS password, an internal attacker with physical access to the SLES wireless client could change the computer boot order, install software, boot an alternate operating system, and take other actions to compromise the wireless client.

In addition, by removing and reading the solid-state drive in the wireless client, critical security-relevant information can be extracted and used to compromise the wireless client.

Recommendations

1. Install tamper-evident systems on SLES wireless and wired clients (such as tamper-evident tape on the wireless client external case, the NVRAM battery, and the solid-state drive) to enhance detection of unauthorized access to internal components; and perform periodic checks to ensure the tamper-evident systems have not been disturbed.
2. Conduct a system engineering trade study to determine the feasibility of installing drive encryption software on SLES wired and wireless clients for operating system and file protection, and implement drive encryption if justified by the trade study.

Assessment of NRC's Wireless Devices

3.3 Autorun Is Enabled on SLES Wireless Clients

Requirement

NIST SP 800-53, Control AC-17 requires that wireless remote access to NRC information systems be authorized, monitored, and controlled.

Finding

The autorun function is enabled on SLES wireless clients for users with administrator access, and partially enabled for users with non-administrator access. Autorun allows executable files on USB drives and external DVD-ROM devices to be launched by the operating system. Autorun is fully functional for administrator accounts on SLES wireless clients, which could lead to unexpected execution of program files on these configuration-controlled machines. In addition, on the evaluated wireless client, when USB drives or external DVD-ROM drives are attached while running under a normal user account (non-administrator), the operating system function opens the device and displays a Windows dialog box that provides a range of user choices depending on the content of the mounted drive. One of these options allows the user to open the device to view the files. Selecting this option opens Windows Explorer, which displays the contents of the drive. It is possible an attacker could place malicious software on the external media and execute it from the Explorer screen. The security principle of least privilege indicates that the function should be removed.

Recommendation

3. Disable autorun on all SLES wireless clients for administrator and user accounts.

3.4 Protection of the SLES Wireless Client Administrative Password Is Inadequate

Requirement

NIST SP 800-53, Control AC-17 requires that wireless remote access to NRC information systems be authorized, monitored, and controlled.

Finding

The administrative password used for the SLES wireless clients is too short to provide sufficient protection from extraction by a technically competent insider threat with physical access. Windows XP passwords that are 14 characters or shorter in length are vulnerable to extraction and decryption.

Recommendation

4. Use administrative passwords for SLES wireless clients that are at least 15 characters long, or configure the Windows XP Embedded operating system on the wireless client to prevent storage of LAN Manager hash password values in the security accounts manager database.

3.5 Detection of SLES Network Scans and Unauthorized Connections to SLES Wireless Access Points Is Inadequate

Requirement

NIST SP 800-53, Control AC-17 requires that wireless remote access to NRC information systems be authorized, monitored, and controlled.

Assessment of NRC's Wireless Devices

Finding

An unauthorized connection was made to an SLES wireless access point using information extracted from an SLES wireless client. This unauthorized connection was not detected and reported.

In addition, using the unauthorized connection to the SLES wireless access point, scans of SLES wireless controllers, switches, routers, and other access points were conducted. These scans were not detected and reported.

Recommendation

5. Deploy an improved detection and reporting process for unauthorized connections to SLES wireless access points and internal scanning activity on SLES.

3.6 Isolation of the SLES Network Is Not Being Verified

Requirement

NIST SP 800-53, Control AC-17 requires that wireless remote access to NRC information systems be authorized, monitored, and controlled.

Finding

SLES is claimed to be air-gapped, logically isolated, and stand-alone in multiple NRC design documents, operations manuals, and procedure documents. However, through document analysis and technical verification, it was determined that SLES is connected to ITI through a firewall connection, and that this connection is used in conjunction with FIPS 140-2 IPSec virtual private network (VPN) connections to provide SLES access to NRC regions. Although the design of this communications architecture is sound and should provide logical isolation of SLES from ITI and the public Internet, there are no technical procedures in place to regularly verify that the security controls are not misconfigured or vulnerable to exploitation. In addition, system administrators and security personnel for SLES and ITI did not know who was responsible for configuration and administration of the connecting firewall.

Recommendation

6. Develop and implement a technical process for isolation verification of SLES from all other connected networks, and provide refresher training to SLES security administrators on organizational responsibility for system configuration and management of SLES security controls for network isolation.

3.7 Awareness of Requirement for Separation of Duties for SLES Is Inadequate

Requirement

NIST SP 800-53, Control AC-5 requires that the personnel who administer and manage wireless access system functions be different from the personnel who establish and manage security policy, procedure, and configurations for wireless access.

Finding

The SLES System Security Plan clearly states that separation of duties is the operational policy for SLES systems management. In addition, the contract structure for security and systems administration for SLES is built to support the principle of separation of duties. However, in interview sessions and during observation of day-to-day operations, it was determined that the security and system administration teams often share duties; and individuals often perform both security and system administration functions in violation of the principle of separation of duties.

Recommendation

7. Provide refresher training for SLES security and system administrators on separation of duties.

3.8 SLES Log Information Is Not Being Consistently Audited

Requirement

NIST SP 800-53, Controls AC-13, AU-1, AU-2 Enhancement 3, and SI-4 require that log information for user, system administration, and access events be audited and managed.

Finding

Audit log information for SLES is being stored and reviewed on an exception basis, but there is no effective process supported by technical systems for reducing, analyzing, and managing auditable events.

Recommendation

8. Evaluate, select, and implement an automated audit log reduction and analysis system for SLES. This system should include both technology and process/procedure elements.

3.9 SLES System Baseline and Change Control Documentation Is Not Managed With Automated Systems

Requirement

NIST SP 800-53, Controls CM-2 Enhancement 2 and CM-3 Enhancement 1 require that system configuration baseline and change documentation be managed with an automated system.

Finding

Although automated systems for managing system baseline and change control information for SLES are required by the control enhancement, this information for SLES is only being managed manually.

Recommendation

9. Evaluate, select, and implement an automated configuration control and baseline documentation system for SLES.

4. FINDINGS - ITI

The assessment identified three notable positive findings for ITI wireless security implementation and nine findings that require remediation. Two findings requiring remediation were related to missing or incomplete high-level policies, and seven were related to implementation or configuration of security controls for ITI wireless access. The findings indicate that ITI is well protected against external penetration and compromise of the Blackberry/BES architecture, and monitoring for unauthorized network-connected wireless access systems is effective. However, several unauthorized network-disconnected wireless access systems were identified during the assessment. These systems could serve as egress points for sensitive information. In addition, they could be connected to desktop systems that are also hard-wired to ITI and could circumvent existing perimeter security controls.

Specific findings for ITI are described below.

4.1 External Security for ITI Wireless Internet-Based Remote Access Is Effective

Requirement

NIST SP 800-53, Control AC-17 requires that wireless remote access to NRC information systems be authorized, monitored, and controlled.

Finding

Wireless Internet-based remote access to ITI is effectively designed, configured, and managed to prevent unauthorized external access to the Blackberry Enterprise Server and associated systems that provide remote access to ITI resources through Blackberry handheld devices. The external connections to these system resources are protected with firewalls, and accessible network services are minimized and effectively configured.

4.2 Detection and Reporting of Unauthorized ITI Network-Connected Wireless Systems Is Effective

Requirement

NIST SP 800-53, Control AC-17 requires that wireless remote access to NRC information systems be authorized, monitored, and controlled.

Finding

A test rogue access point installed on an ITI network connection in an administrative office was quickly detected using internal network techniques, deactivated, and reported.

4.3 Detection and Reporting of Internal ITI Network Scans is Effective

Requirement

NIST SP 800-53, Control AC-17 requires that wireless remote access to NRC information systems be authorized, monitored, and controlled.

Finding

Scanning and network discovery activities intended to identify vulnerabilities in wireless access systems such as the Blackberry Enterprise Server (BES) were quickly discovered by the Office of Information Services (OIS) security team. Quick and appropriate action was taken to deactivate the source network port for the scans and to report the unauthorized activity. During the scans, several exposed services and information sources were detected on the BES and associated systems. Minimal configuration information could be obtained from these systems, but connections to services were refused.

4.4 Detection and Reporting of Unauthorized ITI Network-Disconnected Wireless Systems Is Inadequate

Requirement

NIST SP 800-53, Control AC-17 requires that wireless remote access to NRC information systems be authorized, monitored, and controlled.

Finding

Signal detection and analysis of 802.11 Wi-Fi signals present in OWFN and TWFN identified three radiating Wi-Fi systems with attached client devices. These systems were not verified to be directly connected to ITI due to assessment scope restrictions. For one of these Wi-Fi systems, the encryption technology being used was not identified. For the other two systems, the encryption technology being used was identified as WPA-PSK TKIP, which is an encryption system vulnerable to attack and compromise. These three Wi-Fi systems had not been authorized for installation and operation. In addition, they had not been detected and deactivated.

Several AMX audio-visual control systems that use wireless protocols and a number of wireless printers and other Wi-Fi peripherals were also detected.

Recommendation

10. Implement improved technologies and procedures for detection and management of unauthorized network-disconnected wireless systems. These improvements should include selection and deployment of a wireless intrusion detection system, proactive management of detected wireless systems including wireless printers and audio-visual control systems, policy development and security awareness training for users and administrators related to personal area network (PAN) devices, and refresher training about restrictions on wireless networking systems.

4.5 High-Level Policy for Blackberry-Based Wireless Access to ITI Does Not Exist

Requirement

NIST SP 800-53, Control AC-1 requires a policy statement that defines the purpose, scope, roles, responsibilities, management commitment, coordination, and compliance requirements for wireless Internet-based remote access.

Finding

No high-level policy exists that provides guidance for configuration of the Blackberry Enterprise Servers and Blackberry remote handheld devices. Technical configuration guidelines have been established and implemented, but they were provided by the contractor who installed the Blackberry systems and are not based on a specified organizational policy statement.

Recommendation

11. Revise the NRC Remote E-mail and Wireless Policy addendum to Management Directive 12.5 to include a policy statement that specifies high-level guidance for configuration of the Blackberry-based remote access capability. This policy statement should be general but should include guidance regarding organizational needs for remote access to e-mail, remote access to files and servers, text messaging and other communications functions with handheld devices, and use of handheld devices to provide network connectivity (tethering).

4.6 High-Level Policy for Blackberry Account Management for ITI Does Not Exist

Requirement

NIST SP 800-53, Controls AC-2 and AC-6 require a policy statement that defines requirements for account creation, management, and deletion for wireless Internet-based remote access.

Finding

No high-level policy exists that provides guidance for procedures for Blackberry account management. Account management procedures have been established and implemented, but they are not based on a specific organizational policy.

Recommendation

12. Revise the NRC Remote E-mail and Wireless Policy addendum to Management Directive 12.5 to include a policy statement that provides guidance for Blackberry account management. This policy statement should be general but should include guidance for account creation, deletion, and periodic review. In addition, the policy statement should describe organizational policy for implementing “least privilege” for Blackberry user groups.

4.7 Awareness of Requirement for Separation of Duties for ITI Is Inadequate

Requirement

NIST SP 800-53, Control AC-5 requires that the personnel who administer and manage wireless access system functions be different from the personnel who establish and manage security policy, procedure, and configurations for wireless access.

Finding

The ITI System Security Plan clearly states that separation of duties is the operational policy for ITI systems management. In addition, the contract structure for security and systems administration for ITI is built to support the principle of separation of duties. However, in interview sessions and during observation of day-to-day operations, it was determined that the security and system administration teams often share duties, and individuals often perform both security and system administration functions in violation of the principle of separation of duties.

Recommendation

13. Provide refresher training for ITI security and system administrators on separation of duties.

4.8 ITI Log Information Is Not Being Consistently Audited

Requirement

NIST SP 800-53, Controls AC-13, AU-1, AU-2 Enhancement 3, and SI-4 require that log information for user, system administration, and access events be audited and managed.

Finding

Audit log information for ITI is being stored and reviewed according to policy for security systems, routers, switches, and some servers; but there is no high-level policy or process for reducing and managing audit logs for BES or Exchange servers. An audit log management and review system is in place, but is not being used for BES.

Recommendation

14. Revise and implement procedures for audit log storage and review of BES logs, and use the existing audit log management system to support auditing of BES.

4.9 BES System Settings Are Not Regularly Reviewed for Correctness and Least Functionality

Requirement

NIST SP 800-53, CM-7 Enhancement 1 and SI-7 require that configuration settings for wireless remote access systems be reviewed regularly for least functionality and correctness.

Finding

System configurations for the BES have not been reviewed for least functionality, unnecessary services, and correctness since initial configuration by the installation contractor.

Recommendation

15. Conduct a review of the configuration settings and functions for the BES to ensure only required services are provided and that the configuration is correct and consistent with organizational policy.

4.10 BES System Baseline and Change Control Documentation Is Not Managed With Automated Systems

Requirement

NIST SP 800-53, Controls CM-2 Enhancement 2 and CM-3 Enhancement 1 require that system configuration baseline and change documentation be managed with an automated system.

Finding

An automated system for managing baseline and change control information is being used for most ITI systems as required by the control enhancements. However, based on review of the ITI System Security Plan and observation of operational processes, baseline and change control records for the BES are only being managed manually.

Recommendation

16. Implement a management system to manage BES baseline and change control information.

4.11 BES System Settings Are Not Managed with Automated Tools

Requirement

NIST SP 800-53, Control CM-6 Enhancement 1 requires that configuration settings for wireless remote access systems are managed, documented, and enforced with automated tools.

Finding

Although automated systems for managing system settings are required by the control enhancement, settings for BES are only being managed, documented, and enforced manually.

Recommendation

17. Evaluate, select, and implement an automated server configuration tool for management, documentation, and enforcement of BES server configurations.

4.12 BES Maintenance Records Are Not Managed with Automated Systems

Requirement

NIST SP 800-53, Control MA-2 Enhancement 2 requires that maintenance records for BES be managed with an automated system.

Finding

An automated system for managing maintenance records is being used for most ITI systems as required by the control enhancement. However, although maintenance records for BES are being kept and managed, they are only being managed manually.

Recommendation

18. Implement a maintenance record management system for managing BES maintenance records.

5. OBSERVATIONS

During the assessment, two observations relevant to wireless devices were noted. These observations are provided below.

5.1 Bluetooth Devices

A top-level assessment of Bluetooth-enabled systems was conducted, and multiple active Bluetooth devices were detected in OWFN and TWFN. The detected devices were predominantly Bluetooth-enabled cell phones, but several Bluetooth printers and mouse/keyboard sets were also detected. Existing policy requires that Bluetooth-enabled devices must be approved for use; and in at least one case, according to impromptu interview, there was no review and approval. Although Bluetooth is a short-range technology, it can be easily exploited and can create a pathway for exfiltration of sensitive data. To provide enhanced security, existing policies and training programs for Bluetooth should be reviewed and refreshed.

5.2 Policy Structure

In addition, the overall policy framework that supports both SLES and ITI should be reviewed and revised. The existing policy framework is complex and confusing, and both gaps and overlaps exist. In addition, the traceability between high-level policies (such as the NRC Management Directive documents) and technical policies, procedures, and implementation guidelines for operation and configuration of IT systems is unclear.

6. CONSOLIDATED LIST OF RECOMMENDATIONS

1. Install tamper-evident systems on SLES wireless and wired clients (such as tamper-evident tape on the wireless client external case, the NVRAM battery, and the solid-state drive) to enhance detection of unauthorized access to internal components; and perform periodic checks to ensure the tamper-evident systems have not been disturbed.
2. Conduct a system engineering trade study to determine the feasibility of installing drive encryption software on SLES wired and wireless clients for operating system and file protection, and implement drive encryption if justified by the trade study.
3. Disable autorun on all SLES wireless clients for administrator and user accounts.
4. Use administrative passwords for SLES wireless clients that are at least 15 characters long, or configure the Windows XP Embedded operating system on the wireless client to prevent storage of LAN Manager hash password values in the security accounts manager database.
5. Deploy an improved detection and reporting process for unauthorized connections to SLES wireless access points and internal scanning activity on SLES.
6. Develop and implement a technical process for isolation verification of SLES from all other connected networks, and provide refresher training to SLES security administrators on organizational responsibility for system configuration and management of SLES security controls for network isolation.
7. Provide refresher training for SLES security and system administrators on separation of duties.
8. Evaluate, select, and implement an automated audit log reduction and analysis system for SLES. This system should include both technology and process/procedure elements.
9. Evaluate, select, and implement an automated configuration control and baseline documentation system for SLES.
10. Implement improved technologies and procedures for detection and management of unauthorized network-disconnected wireless systems. These improvements should include selection and deployment of a wireless intrusion detection system, proactive management of detected wireless systems including wireless printers and audio-visual control systems, policy development and security awareness training for users and administrators related to personal area network (PAN) devices, and refresher training about restrictions on wireless networking systems.
11. Revise the NRC Remote E-mail and Wireless Policy addendum to Management Directive 12.5 to include a policy statement that specifies high-level guidance for configuration of the Blackberry-based remote access capability. This policy statement should be general but should include guidance regarding organizational needs for remote access to e-mail, remote access to files and servers, text messaging and other communications functions with handheld devices, and use of handheld devices to provide network connectivity (tethering).
12. Revise the NRC Remote E-mail and Wireless Policy addendum to Management Directive 12.5 to include a policy statement that provides guidance for Blackberry account management. This policy statement should be general but should include guidance for account creation, deletion, and periodic review. In addition, the policy statement should describe organizational policy for implementing “least privilege” for Blackberry user groups.
13. Provide refresher training for ITI security and system administrators on separation of duties.
14. Revise and implement procedures for audit log storage and review of BES logs, and use the existing audit log management system to support auditing of BES.

Assessment of NRC's Wireless Devices

15. Conduct a review of the configuration settings and functions for the BES to ensure only required services are provided and that the configuration is correct and consistent with organizational policy.
16. Implement a management system to manage BES baseline and change control information.
17. Evaluate, select, and implement an automated server configuration tool for management, documentation, and enforcement of BES server configurations.
18. Implement a maintenance record management system for managing BES maintenance records.

7. AGENCY COMMENTS

At an exit conference held on September 7, 2010, agency management stated their general agreement with the findings and recommendations in this report. Agency management also provided supplemental information that has been incorporated into this report as appropriate. As a result, the agency opted not to provide formal comments for inclusion in this report.

~~OFFICIAL USE ONLY – SECURITY RELATED INFORMATION~~

Assessment of NRC's Wireless Devices

APPENDIX

~~OFFICIAL USE ONLY – SECURITY RELATED INFORMATION~~

APPENDIX A. ASSESSMENT SCOPE AND METHODOLOGY

The wireless assessment focused on security policies and procedures, current technology deployment, operational capabilities, and system configurations for wireless network access. Southwest Research Institute (SwRI) performed the assessment in three stages:

1. Documentation review of policy, procedure, and technical configurations
2. On-site familiarization and network discovery, including interviews with critical stakeholders
3. On-site technical security assessment of wireless network access systems and controls

First, SwRI reviewed executive orders, public law, and high-level guidance from organizations such as the Office of Management and Budget (OMB), the Government Accountability Office (GAO), and the National Institute of Standards and Technology (NIST) to determine the policy framework for Nuclear Regulatory Commission (NRC) Office of the Inspector General (OIG) audits and NRC operations. Based on this external framework, SwRI analyzed high-level guidance in the NRC Management Directives (MDs), technical policy and procedures documentation for each of the two systems being assessed, job aids, operational guidance, and other documentation to determine compliance with external requirements, existing executive-level guidance at NRC, and best practices. Based on this analysis, SwRI documented gaps, inconsistencies, and errors in the policy framework.

SwRI also collected and analyzed network documentation, as-built drawings, and existing wireless operations documents. SwRI reviewed this technical documentation to identify potential security weaknesses and identify areas for further on-site evaluation during the assessment. Information from the documentation review was incorporated into the assessment plan before the on-site assessment began.

Following the documentation review, SwRI performed Site Visit 1. During Site Visit 1, SwRI reviewed the existing network infrastructure and gathered technical information important to the assessment process. SwRI conducted a site visit kickoff meeting to meet the appropriate contacts and stakeholders to set expectations and answer questions. In subsequent meetings, SwRI interviewed key stakeholders to gather further policy and technical information to answer questions generated from the initial documentation review. SwRI used software tools such as nmap to discover the existing network architecture and topology for the networks. Based on the information gathered during Site Visit 1, the assessment team determined that the following major areas would constitute the assessment:

1. One White Flint North (OWFN) and Two White Flint North (TWFN) administrative network – analysis and assessment to verify that no wireless capability or rogue access points exist for 802.11x access to the network, according to current policy
2. OWFN and TWFN administrative network – analysis and assessment to verify that Internet-based remote access to the administrative network using mobile wireless devices (i.e., BlackBerry access through BlackBerry Enterprise Server) follows existing policy guidelines and best practices
3. Safeguards LAN and eSafe (SLES) system – technical assessment to verify that 802.11x access to SLES follows existing policy guidelines and best practices
4. OWFN and TWFN administrative network and SLES – top-level review of policy and implementation for Bluetooth devices

During the second site visit, SwRI performed the security assessment of wireless access capabilities, including analysis of both remote access through 802.11 access points and access

Assessment of NRC's Wireless Devices

through cellular connections from wireless handheld devices such as smart phones and PDAs. SwRI used software and hardware tools including:

- aircap
- Kismet
- Global Positioning System (GPS) receiver
- Visiwave site scanning mapping software
- Channelizer signal analysis device
- Network discovery and analysis tool suites: metasploit and Back Track

These components were used to detect and document existing 802.11 wireless access points to the network to provide an “outside-in” perspective to the exposed nodes of the network. In addition, SwRI analyzed server and handheld configurations to characterize BES configurations, handheld controls and capabilities, and connections to both the internal Exchange servers and external RIM servers. SwRI provided an outbrief for NRC OIG and agency personnel to outline initial findings and discuss recommendations.